Conversion Guide

Configuration Converter to USG FLEX H series

Version 6.2.0 edition 1

July 7, 2026

Contents

Introduction

Key Benefits

The Configuration Converter helps organizations streamline platform upgrades and reduce migration complexity when moving to newer Zyxel security appliances.

Key benefits include:

- **Reduce Migration Time**
  Automatically converts supported configurations, eliminating the need to manually recreate network and security settings.
- **Minimize Configuration Errors**
  Reduces the risk of human errors commonly introduced during manual migration.
- **Preserve Existing Security Policies**
  Retains supported firewall, NAT, VPN, routing, and network configurations to help maintain service continuity.
- **Simplify Hardware Refresh Projects**
  Enables a smoother transition from legacy USG, ZyWALL, VPN, ATP and USG FLEX platforms to newer USG FLEX H series devices.
- **Accelerate Deployment**
  Allows administrators to focus on validation and optimization rather than rebuilding configurations from scratch.
- **Provide Migration Visibility**
  Generates detailed conversion reports, warnings, and error messages to help identify configuration items requiring manual review.

Purpose of Configuration Converter

The Configuration Converter is designed to simplify the migration process between Zyxel security appliance platforms by automatically translating supported configuration settings from a source device to a target device.

The converter helps preserve existing network, security, and VPN configurations during hardware upgrades, reducing manual reconfiguration effort and minimizing migration time.

Because hardware architectures, firmware capabilities, and feature availability may differ between platforms, some settings may be modified, partially converted, or excluded during the conversion process. After the conversion is completed, administrators should review the conversion report and verify the converted configuration before deployment.

The Configuration Converter is intended to assist migration projects and should be used as part of a planned migration process. Final configuration validation and testing remain the responsibility of the administrator.

Supported Migration Paths

The Configuration Converter supports migration between selected Zyxel security appliance product families, including legacy USG and ZyWALL platforms and newer ATP, VPN, USG FLEX, and USG FLEX H series devices.

Supported migration scenarios include:

- USG → ATP Series
- USG → USG FLEX Series
- USG → USG FLEX H Series
- ZyWALL → VPN Series
- ZyWALL → USG FLEX Series
- ZyWALL → USG FLEX H Series
- ATP → USG FLEX H Series
- USG FLEX → USG FLEX H Series
- VPN → USG FLEX H Series

The converter automatically maps supported configuration objects, interfaces, policies, and VPN settings based on the selected source and target platforms.

Please refer to the **Supported Upgrade Paths** section for the complete model compatibility matrix and recommended migration paths.

Wireless Model Considerations

When migrating between wireless and non-wireless models, WiFi-related configurations require special attention:

- **Wireless to Non-Wireless Models**

Wireless settings, SSIDs, radio profiles, and related WiFi configurations are not migrated.

- **Non-Wireless to Wireless Models**

  Wireless functionality is supported on the target device; however, WiFi settings must be configured manually after migration.

Administrators should review wireless configurations separately after completing the conversion process.

Supported Upgrade Paths

The configuration converter supports converting Zyxel security appliances to USG FLEX H series. Please refer to the supported model correspondence table.

Source Model	★ Recommended Upgrade (Primary Path)	Alternative Upgrade Options
USG FLEX 50 (USG20-VPN)	USG FLEX 50H / 50HP	—
USG20W-VPN*	USG FLEX 50H / 50HP	—
USG FLEX 50AX*	USG FLEX 50H / 50HP	—
USG FLEX 100	USG FLEX 100H / 100HP	—
USG FLEX 100W*	USG FLEX 100H / 100HP	—
USG FLEX 100AX*	USG FLEX 100H / 100HP	—
USG FLEX 200	USG FLEX 200H / 200HP	—
USG FLEX 500	USG FLEX 500H	—
USG FLEX 700	USG FLEX 700H	—
ATP100	USG FLEX 100H / 100HP	—
ATP100W*	USG FLEX 100H / 100HP	—
ATP200	USG FLEX 200H / 200HP	—
ATP500	USG FLEX 500H	—
ATP700	USG FLEX 700H	—
ATP800	USG FLEX 700H	—
VPN50	USG FLEX 100H / 100HP	—
VPN100	USG FLEX 200H / 200HP	—
VPN300	USG FLEX 500H	—
VPN1000	USG FLEX 700H	—
USG40	USG FLEX 50H / 50HP	USG FLEX 100 / ATP100
USG40W*	USG FLEX 50H / 50HP	USG FLEX 100W / ATP100W
USG60	USG FLEX 100H / 100HP	USG FLEX 200 / ATP100
USG60W*	USG FLEX 100H / 100HP	USG FLEX 200 / ATP100W
USG110	USG FLEX 200H / 200HP	USG FLEX 500 / ATP200
USG210	USG FLEX 200H / 200HP	USG FLEX 500 / ATP200
USG310	USG FLEX 500H	USG FLEX 700 / ATP500
USG1100	USG FLEX 700H	ATP800 / ATP700
USG1900	USG FLEX 700H	ATP800 / ATP700
ZyWALL 110	USG FLEX 200H / 200HP	USG FLEX 500 / VPN100
ZyWALL 310	USG FLEX 500H	USG FLEX 700 / VPN300
ZyWALL 1100	USG FLEX 700H	VPN1000

*** Wireless Model Considerations:**

- Wireless → Non-Wireless: WiFi settings are not migrated.
- Non-Wireless → Wireless: WiFi settings must be configured manually.

Before You Start

Zyxel Converter is a migration tool, not a migration service. It is designed to be utilized as part of a properly planned migration process.
To ensure a successful conversion and prevent device lockout, please review and complete the following prerequisites before starting the conversion.

Please review the following requirements before starting the conversion:

1. **Encrypted Configurations (Sensitive Data Protection)**
   Some devices support **Sensitive Data Protection**, which uses a **Private Encryption Key** to protect locally stored user passwords.

   When this feature is enabled:
   - Local user passwords are encrypted using the Private Encryption Key
   - Encrypted values are shown in CLI and configuration files in encoded form
   - The Private Encryption Key is required when restoring a configuration backup

   Before conversion, you must **remove the Private Encryption Key from the configuration file** and export the updated configuration again.

   Important:
   If the Private Encryption Key is not removed before conversion, the converted configuration may be applied to the new platform, but the administrator will **be unable to log in** using the original password.

2. **File Naming**
   The uploaded configuration filename must be **fewer than 40 characters**, as this name will be used for the converted policy package.
   File name format: {original file name 40 characters}_converted-XXXXXX.conf
   XXXXXX is a serial number that generated automatically.

Example: usg110-2026aprilproject_converted-123456.conf

   English only. The valid characters are [a-zA-Z0-9~_=-].

3. **Firmware Compatibility**
   When migrating from ATP/USG FLEX, ensure you are using the latest ZLD OS firmware available on the portal (ZLD **V5.37 or later** is highly recommended).

4. **Configuration Parameter Limits**

The converter validates configurations against maximum parameter limits. If these limits are exceeded, the conversion will fail and generate a detailed error log.

Post-Conversion Notice

After conversion, please review the generated log file to verify all changes applied during the conversion process.

Static Port/Interface Mapping

uOS Platform

The USG FLEX H series (uOS platform) has an interface name length limit of **11** characters.

- If the user-defined interface name is within the limit, it will be directly used and displayed as the interface name.
- If the user-defined interface name exceeds the limit, the uOS interface name will consist of the user-defined name followed by a serial number, truncated to 11 characters in total. The full user-defined name will be moved to the Description field.
- If the Description field already contains a value, the original user-defined description will take precedence over the interface name.

Strategic Architectural Details:

- SFP Port Conversion Strategy

Four strategic approaches are adopted for SFP port handling:

1. **Convert to Optional Port (opt)** — maximize deployment flexibility
2. **Convert to Secondary WAN (wan2)** — standardize dual-WAN architecture
3. **Convert to RJ45 general Port** — preserve HA heartbeat architecture
4. **Bypass SFP Port Conversion (No Conversion)**— no conversion for the SFP port

- Interface Mapping

1. Fixed-Zone Models: Interfaces are automatically remapped to match the target platform's predefined interface layout.
2. Configurable-Zone Models: Original interface assignments are preserved using 1:1 port mapping whenever possible.

Pxx indicates to the physical ports.
(xxx) indicates to the port role- zone Interface.
if all the ports are configurable then there is no (xxx) specific zone interface.

Legacy model to USG FLEX 50H/HP

USG FLEX 50 / USG20W-VPN	P1(sfp)	P2(wan)	P3(lan1)	P4(lan1)	P5(lan1)	P6(opt)
USG FLEX 50H/HP		P1(wan)	P2(lan1)	P3(lan1)	P4(lan1)	P5(opt)

USG40(W)		P1(wan1)	P2(lan1)	P3(lan2)	P4(dmz)	P5(opt)
USG FLEX 50AX		P1(wan)	P2(lan1)	P3(lan2)	P4(dmz)	P5(opt)
USG FLEX 50H/HP		P1(wan)	P2(lan1)	P3(lan2)	P4(dmz)	P5(opt)

Legacy model to USG FLEX 100H/HP

ATP100(W)		P2(wan)	P3(lan1)	P4(lan1)	P5(lan1)	P6(opt)		
USG FLEX 100(W)	P1(sfp)	P2(wan)	P3(lan1)	P4(lan1)	P5(lan1)	P6(opt)		
USG FLEX 100H/HP	P1(ge1)	P2(wan)	P3(lan1)	P4(lan1)	P5(lan1)	P6(opt)	P7	P8

USG FLEX 100AX	P1(wan)	P2(lan1)	P3(lan2)	P4(dmz)	P5(opt)			
USG FLEX 100H/HP	P1(wan)	P2(lan1)	P3(lan2)	P4(dmz)	P5(opt)	P6	P7	P8

VPN50	P1(sfp)	P2(wan)	P3(lan1)	P4(lan2)	P5(dmz)	P6(opt)		
USG FLEX 100H/HP	P1(ge1)	P2 (wan)	P3(lan1)	P4(lan2)	P5(dmz)	P6(opt)	P7	P8

The USG60(W) port 2 (wan2) will be mapped to USG FLEX 100H/HP port 1.

USG60(W)	P1(wan1)	P2(wan2)	P3(lan1)	P4(lan2)	P5(dmz)	P6(guest)		
USG FLEX 100H/HP	P1(wan2)	P2(wan1)	P3(lan1)	P4(lan2)	P5(dmz)	P6(guest)	P7	P8

Legacy model to USG FLEX 200H/HP

res.=reserved

USG FLEX/ATP200 Series	P1(sfp)	P2(wan1)	P3(wan2)	P4(lan1)	P5(lan1)	P6(lan1)	P7(res.)	
VPN100	P1(sfp)	P2(wan1)	P3(wan2)	P4(lan1)	P5(lan1)	P6(lan1)	P7(res.)	
USG FLEX 200H/HP	P1(ge1)	P2(wan1)	P3(wan2)	P4(lan1)	P5(lan1)	P6(lan1)	P7 (res.)	P8

USG60(W)		P1(wan1)	P2(wan2)	P3(lan1)	P4(lan2)	P5(dmz)	P6(guest)	
USG FLEX 200H/HP	P1(ge1)	P2(wan1)	P3(wan2)	P4(lan1)	P5(lan2)	P6(dmz)	P7 (guest)	P8

res.=reserved

USG110/210 ZyWALL 110	P1(wan1)	P2(wan2)	P3(opt)	P4(lan1)	P5(lan2)	P6(res.)	P7(dmz)	
USG FLEX 200H/HP	P1(opt)	P2(wan1)	P3(wan2)	P4(lan1)	P5(lan2)	P6(dmz)	P7 (res.)	P8

Legacy model to USG FLEX 500H

USG FLEX /ATP500 Series	P1	P2	P3	P4	P5	P6	P7	P8				
VPN300	P1	P2	P3	P4	P5	P6	P7	P8				
USG FLEX 500H	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12

ZyWALL/USG310	P1	P2	P3	P4	P5	P6	P7	P8				
USG FLEX 500H	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12

Port 3 (OPT) is converted to Port 1, removed from the OPT group, and reassigned to WAN2 after conversion.

USG110/210	P1(wan1)	P2(wan2)	P3(opt)	P4(lan1)	P5(lan2)	P6 (Res.)	P7(dmz)					
USG FLEX 500H	P1 (opt)	P2 (wan1)	P3 (wan2)	P4 (lan1)	P5 (lan2)	P6 (dmz)	P7 (res.)	P8	P9	P10	P11	P12

Legacy model to USG FLEX 700H

The ports on the USG FLEX/ATP700, ATP800, and VPN1000 are configurable. The converter preserves the original interface assignments by performing 1:1 port mapping whenever possible.

ATP700/800 USG FLEX 700 VPN1000 Series	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14
USG FLEX 700H	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14

ZyWALL 310/1100 USG310/1100/1900	P1	P2	P3	P4	P5	P6	P7	P8						
USG FLEX 700H	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14

Conversion Scopes

The Zyxel Configuration Converter supports migration of selected configuration settings between platforms. Due to differences in product architecture and feature implementation, some configurations may be partially converted or excluded.

After completing the conversion, please review the generated conversion log file to identify all changes, skipped items, and configurations requiring manual adjustment.

Supported Features

Supported: The converter is capable of translating configurations for the following:

1. **Supported Components:** The converter is capable of translating configurations for the following:
    - **Interface:** Physical interfaces, logical interfaces, and PPPoE interfaces
    - **Objects:** Addresses, Address Groups, Services, Service Groups, Schedule, and Schedule Groups
    - **Users:** Local Users and User Groups
    - **Policies:** NAT, Firewall, and Route Policies
    - **Networking :** DHCP (Server, Client, and Relay)
    - **VPN:** IPSEC IKEv2 site-to-site, SSL VPN profile
    - **Security Features:** Due to architectural differences between platforms, the following features may require manual review or post-conversion adjustments. For detailed information on how each feature is handled, please refer to the "**Security Feature Limitations**" section of the Converter User Guide:
        (1) Application Patrol
        (2) Content Filtering
        (3) Reputation Filter
        (4) Anti-Malware
        (5) Sandboxing
        (6) IPS
        (7) IP Exception
        (8) SSL Inspection
        (9) External Block List

Unsupported Features

1. **IPv6:** This converter currently only supports **IPv4 objects and rules**. All IPv6-specific objects and rules will be ignored during the process.
2. **Security Credentials:** Private keys and certificates will not be migrated. The system will revert to using the **default certificate** upon completion.
3. **Schedules:** Schedule-related settings are not supported. This includes:
   - Scheduled configuration backups
   - Firmware upgrades
   - Signature/certificate updates.
4. **Mail Server Settings:** Mail server settings—including those for Syslog, Daily Email Reports, and Event Alerts—will not be converted and must be reconfigured manually.
5. **Licenses Services:** all licenses will not be migrated and must be reassigned after conversion.

Configuration Parameter Limits

The converter validates configuration parameters to ensure they comply with the supported limits of the target platform.

If a parameter exceeds the supported limit, the converter will attempt to truncate the value and continue the conversion whenever possible. If truncation is not possible, the conversion may stop and require manual intervention.

Configurations that exceed the supported limits may result in:

- Conversion failure
- An incomplete converted configuration file
- Failure when applying the converted configuration to the target device

After the conversion is complete, review all warning and error messages to identify any items that require manual adjustment before deploying the converted configuration.

When an error occurs:

- The message will identify the related rule, object, or parameter that caused the issue.
- The generated configuration file may be incomplete and **must not be used on the target device.**

Target model is 50H series

	Source	Source	Source	Source	Target
Model	**USG40 series**	**USG FLEX 100 series**	**ATP100 series**	**VPN50**	**USG FLEX 50H/HP**
Max. number of IPsec VPN tunnel	20	50	50	50	20
Max. bridge interface (physical port: Eth+ SFP /2)	2	2	2	2	2
Max. policy route rules	100	100	100	100	100
Max. user define trunk	4	4	4	4	4
Max. NAT virtual server number	128	128	128	128	64
Max. session limit per host rules (Firewall)	1000	1000	1000	1000	100
Max. address object number	300	300	300	300	300
Max. service object number	200	200	200	200	200
Max. schedule object number	32	32	32	32	32
Max. application object number	500	500	500	500	500
Max. LDAP server object number	2	2	2	2	4
Max. Radius server object number	2	2	2	2	4
Max. AD server object number	4	2	2	2	4
Max. A record number	32	64	64	64	32
Max. NS record number	8	8	8	8	8
Max. MX record number	4	8	8	4	4
Max. DHCP network pool (vlan+brg+ethernet)	14	15	15	15	15
Max. DHCP options (pre-defined + user defined) (per pool)	10	10	10	10	15
Max. number of Content Filtering profiles	16	16	16	16	16
Max. number of Application Patrol profiles	N/A	32	32	N/A	32
Max. URL Threat Filter allow list rule	N/A	1024	1024	N/A	256
Max. URL Threat Filter block list rule	N/A	1024	1024	N/A	256
Max. DNS Threat Filter allow list rule	N/A	1024	1024	N/A	256
Max. DNS Threat Filter block list rule	N/A	1024	1024	N/A	256

Target model is 100H series

	Source	Source	Source	Source	Target
Model	**USG40 series**	**USG FLEX 100 series**	**ATP100 series**	**VPN50**	**USG FLEX 100H/HP**
Max. number of IPsec VPN tunnel	20	50	50	50	50
Max. bridge interface (physical port: Eth+ SFP /2)	2	2	2	2	4
Max. policy route rules	100	100	100	100	100
Max. user define trunk	4	4	4	4	4
Max. NAT virtual server number	128	128	128	128	64
Max. session limit per host rules (Firewall)	1000	1000	1000	1000	100
Max. address object number	300	300	300	300	300
Max. service object number	200	200	200	200	200
Max. schedule object number	32	32	32	32	32
Max. application object number	500	500	500	500	500
Max. LDAP server object number	2	2	2	2	4
Max. Radius server object number	2	2	2	2	4
Max. AD server object number	4	2	2	2	4
Max. A record number	32	64	64	64	64
Max. NS record number	8	8	8	8	8
Max. MX record number	4	8	8	4	8
Max. DHCP network pool (vlan+brg+ethernet)	14	15	15	15	28
Max. DHCP options (pre-defined + user defined) (per pool)	10	10	10	10	15
Max. number of Content Filtering profiles	16	16	16	16	16
Max. number of Application Patrol profiles	N/A	32	32	N/A	32
Max. URL Threat Filter allow list rule	N/A	1024	1024	N/A	256
Max. URL Threat Filter block list rule	N/A	1024	1024	N/A	256
Max. DNS Threat Filter allow list rule	N/A	1024	1024	N/A	256
Max. DNS Threat Filter block list rule	N/A	1024	1024	N/A	256

	Source	Target
Model	**USG60 series**	**USG FLEX 100H/HP**
Max. number of IPsec VPN tunnel	40	50
Max. bridge interface (physical port: Eth+ SFP /2)	4	4
Max. policy route rules	200	100
Max. user define trunk	4	4
Max. NAT virtual server number	256	64
Max. session limit per host rules (Firewall)	1000	100
Max. address object number	300	300
Max. service object number	200	200
Max. schedule object number	32	32
Max. application object number	500	500
Max. LDAP server object number	2	4
Max. Radius server object number	2	4
Max. AD server object number	4	4
Max. A record number	64	64
Max. NS record number	8	8
Max. MX record number	8	8
Max. DHCP network pool (vlan+brg+ethernet)	24	28
Max. DHCP options (pre-defined + user defined) (per pool)	10	15
Max. number of Content Filtering profiles	16	16
Max. number of Application Patrol profiles	N/A	32
Max. URL Threat Filter allow list rule	N/A	256
Max. URL Threat Filter block list rule	N/A	256
Max. DNS Threat Filter allow list rule	N/A	256
Max. DNS Threat Filter block list rule	N/A	256

Target model is 200H series

	Source	Source	Source	Source	Target
Model	**USG60 series**	**USG FLEX 200**	**ATP200**	**VPN100**	**USG FLEX 200H/HP**
Max. number of IPsec VPN tunnel	40	100	100	100	100
Max. bridge interface (physical port: Eth+ SFP /2)	4	8	8	8	4
Max. policy route rules	200	500	500	500	100
Max. user define trunk	4	8	8	4	4
Max. NAT virtual server number	256	256	256	256	128
Max. session limit per host rules (Firewall)	1000	1000	1000	1000	100
Max. address object number	300	300	300	300	300
Max. service object number	200	500	500	500	500
Max. schedule object number	32	32	32	32	32
Max. application object number	500	500	500	500	500
Max. LDAP server object number	2	8	8	8	4
Max. Radius server object number	2	8	8	8	4
Max. AD server object number	4	8	8	8	4
Max. A record number	64	64	64	64	64
Max. NS record number	8	16	16	16	8
Max. MX record number	8	8	8	8	8
Max. DHCP network pool (vlan+brg+ethernet)	24	29	29	29	44
Max. DHCP options (pre-defined + user defined) (per pool)	10	15	15	15	15
Max. number of Content Filtering profiles	16	16	16	16	16
Max. number of Application Patrol profiles	N/A	32	32	N/A	32
Max. URL Threat Filter allow list rule	N/A	1024	1024	N/A	256
Max. URL Threat Filter block list rule	N/A	1024	1024	N/A	256
Max. DNS Threat Filter allow list rule	N/A	1024	1024	N/A	256
Max. DNS Threat Filter block list rule	N/A	1024	1024	N/A	256

	Source	Source	Target
Model	**ZyWALL / USG110**	**USG210**	**USG FLEX 200H/HP**
Max. number of IPsec VPN tunnel	100	200	100
Max. bridge interface (physical port: Eth+ SFP /2)	8	8	4
Max. policy route rules	500	500	100
Max. user define trunk	8	8	4
Max. NAT virtual server number	256	512	128
Max. session limit per host rules (Firewall)	1000	1000	100
Max. address object number	300	500	300
Max. service object number	500	500	500
Max. schedule object number	32	32	32
Max. application object number	500	500	500
Max. LDAP server object number	8	8	4
Max. Radius server object number	8	8	4
Max. AD server object number	8	8	4
Max. A record number	64	64	64
Max. NS record number	16	16	8
Max. MX record number	8	8	8
Max. DHCP network pool (vlan+brg+ethernet)	29	45	44
Max. DHCP options (pre-defined + user defined) (per pool)	15	15	15
Max. number of Content Filtering profiles	16	16	16
Max. number of Application Patrol profiles	N/A	N/A	32
Max. URL Threat Filter allow list rule	N/A	N/A	256
Max. URL Threat Filter block list rule	N/A	N/A	256
Max. DNS Threat Filter allow list rule	N/A	N/A	256
Max. DNS Threat Filter block list rule	N/A	N/A	256

Target model is 500H

	Source	Source	Source	Target
Model	**USG FLEX 500**	**ATP500**	**VPN300**	**USG FLEX 500H**
Max. number of IPsec VPN tunnel	300	300	300	300
Max. bridge interface (physical port: Eth+ SFP /2)	16	16	16	6
Max. policy route rules	500	500	500	300
Max. user define trunk	16	16	16	8
Max. NAT virtual server number	1024	1024	1024	256
Max. session limit per host rules (Firewall)	1000	1000	1000	100
Max. address object number	1000	1000	1000	500
Max. service object number	1000	1000	1000	1000
Max. schedule object number	32	32	32	32
Max. application object number	1000	1000	1000	1000
Max. LDAP server object number	16	16	16	8
Max. Radius server object number	16	16	16	8
Max. AD server object number	16	16	16	8
Max. A record number	128	128	128	128
Max. NS record number	16	16	16	8
Max. MX record number	16	16	16	8
Max. DHCP network pool (vlan+brg+ethernet)	88	88	88	82
Max. DHCP options (pre-defined + user defined) (per pool)	30	15	30	15
Max. number of Content Filtering profiles	32	32	32	32
Max. number of Application Patrol profiles	64	64	N/A	64
Max. URL Threat Filter allow list rule	1024	1024	N/A	256
Max. URL Threat Filter block list rule	1024	1024	N/A	256
Max. DNS Threat Filter allow list rule	1024	1024	N/A	256
Max. DNS Threat Filter block list rule	1024	1024	N/A	256

	Source	Source	Source	Target
Model	**ZyWALL / USG110**	**USG210**	**ZyWALL / USG310**	**USG FLEX 500H**
Max. number of IPsec VPN tunnel	100	200	300	300
Max. bridge interface (physical port: Eth+ SFP /2)	8	8	16	6
Max. policy route rules	500	500	1000	300
Max. user define trunk	8	8	16	8
Max. NAT virtual server number	256	512	1024	256
Max. session limit per host rules (Firewall)	1000	1000	1000	100
Max. address object number	300	500	1000	500
Max. service object number	500	500	1000	1000
Max. schedule object number	32	32	32	32
Max. application object number	500	500	1000	1000
Max. LDAP server object number	8	8	16	8
Max. Radius server object number	8	8	16	8
Max. AD server object number	8	8	16	8
Max. A record number	64	64	128	128
Max. NS record number	16	16	16	8
Max. MX record number	8	8	16	8
Max. DHCP network pool (vlan+brg+ethernet)	29	45	88	82
Max. DHCP options (pre-defined + user defined) (per pool)	15	15	30	15
Max. number of Content Filtering profiles	16	16	32	32
Max. number of Application Patrol profiles	N/A	N/A	N/A	64
Max. URL Threat Filter allow list rule	N/A	N/A	N/A	256
Max. URL Threat Filter block list rule	N/A	N/A	N/A	256
Max. DNS Threat Filter allow list rule	N/A	N/A	N/A	256
Max. DNS Threat Filter block list rule	N/A	N/A	N/A	256

Target model is 700H

	Source	Source	Source	Source	Target
Model	**USG FLEX 700**	**ATP700**	**ATP800**	**VPN1000**	**USG FLEX 700H**
Max. number of IPsec VPN tunnel	500	500	1000	1000	1000
Max. bridge interface (physical port: Eth+ SFP /2)	16	16	16	16	7
Max. policy route rules	1000	1000	1000	1000	500
Max. user define trunk	32	32	32	32	8
Max. NAT virtual server number	1024	1024	1024	1024	512
Max. session limit per host rules (Firewall)	1000	1000	1000	1000	100
Max. address object number	2000	2000	2000	2000	1500
Max. service object number	1000	1000	1000	1000	1000
Max. schedule object number	32	32	32	32	32
Max. application object number	1000	1000	1000	1000	1000
Max. LDAP server object number	16	16	16	16	8
Max. Radius server object number	16	16	16	16	8
Max. AD server object number	16	16	16	16	8
Max. A record number	128	128	128	128	128
Max. NS record number	16	16	16	16	8
Max. MX record number	16	16	16	16	8
Max. DHCP network pool (vlan+brg+ethernet)	158	158	158	158	147
Max. DHCP options (pre-defined + user defined) (per pool)	30	30	30	30	15
Max. number of Content Filtering profiles	64	64	64	64	32
Max. number of Application Patrol profiles	96	96	96	N/A	96
Max. URL Threat Filter allow list rule	1024	1024	1024	N/A	256
Max. URL Threat Filter block list rule	1024	1024	1024	N/A	256
Max. DNS Threat Filter allow list rule	1024	1024	1024	N/A	256
Max. DNS Threat Filter block list rule	1024	1024	1024	N/A	256

	Source	Source	Source	Target
Model	**ZyWALL / USG310**	**ZyWALL / USG1100**	**USG1900**	**USG FLEX 700H**
Max. number of IPsec VPN tunnel	300	1000	2000	1000
Max. bridge interface (physical port: Eth+ SFP /2)	16	16	16	7
Max. policy route rules	1000	1000	2000	500
Max. user define trunk	16	32	32	8
Max. NAT virtual server number	1024	1024	1024	512
Max. session limit per host rules (Firewall)	1000	1000	1000	100
Max. address object number	1000	2000	2000	1500
Max. service object number	1000	1000	1000	1000
Max. schedule object number	32	32	32	32
Max. application object number	1000	1000	1000	1000
Max. LDAP server object number	16	16	16	8
Max. Radius server object number	16	16	16	8
Max. AD server object number	16	16	16	8
Max. A record number	128	128	128	128
Max. NS record number	16	16	16	8
Max. MX record number	16	16	16	8
Max. DHCP network pool (vlan+brg+ethernet)	88	152	152	147
Max. DHCP options (pre-defined + user defined) (per pool)	30	30	30	15
Max. number of Content Filtering profiles	32	64	128	32
Max. number of Application Patrol profiles	N/A	N/A	N/A	96
Max. URL Threat Filter allow list rule	N/A	N/A	N/A	256
Max. URL Threat Filter block list rule	N/A	N/A	N/A	256
Max. DNS Threat Filter allow list rule	N/A	N/A	N/A	256
Max. DNS Threat Filter block list rule	N/A	N/A	N/A	256

Limitations for uOS Platform

This chapter explains the precautions, behaviors, and limitations of the converter for each feature and function.

Networking

- **Link Aggregation Group (LAG), Bridge, GRE,** and **Virtual Interfaces** are not supported. Remove any LAG, GRE or Bridge configurations before starting the conversion.
- **IPv6** configurations are not supported for conversion.
- **Application Layer Gateway (ALG)** settings for **H.323** are not supported and will not be converted.
- **DNS Zone Forwarding** configurations are not supported for conversion.
- **DNS Security** options converts only address objects of the **'host'** or **'subnet'** types; other types will not be converted.
- **PPTP** and **L2TP** are not supported. If the source configuration contains PPTP or L2TP settings, any related parameters that map to supported configuration fields are retained and displayed in the target device's UI. However, these settings are inactive and will not take effect.

Interface

- The converter does not support SFP interfaces. After conversion, SFP interfaces will be changed to General interfaces, and related interfaces (e.g., sfp_ppp) will be removed.
- Conversion from virtual interface to secondary IP is not supported.
- Connectivity Check conversion notice for External Interfaces, the converter does not support "Check Default Gateway" in Connectivity Check settings.
    - If the original configuration uses this option, it cannot be directly converted or function as expected.
    - During conversion, this setting will be translated to "Check These Addresses" with the value **‘default-gateway’**, and **Connectivity Check will be disabled by default**.
    - This indicates the setting originated from "Check Default Gateway".
    - Please review the converted configuration file and **manually adjust the Connectivity Check settings as needed** to ensure they meet your deployment requirements.

Routing

- Dynamic routing protocols, including RIP, OSPF, and BGP, are not supported for conversion.

NAT Rules

- NAT rules will not be created for Fully Qualified Domain Name (FQDN) objects.

Site-to-Site VPN

- IPsec VPN does not support converting IKEv1 xAuth configurations.
- IPsec VPN connection rules containing DNAT or SNAT will not be converted.
- IPsec VPN certificates will revert to uOS default settings; users must review and reconfigure their IPsec VPN settings after conversion.
- IPsec VPN local/remote policy does not support address object types “range,” “interface-subnet,” “interface-IP,” or “interface-gateway,” and these cannot be converted.

Remote Access IPSEC VPN

- Only one policy will be converted. If created using the wizard, that policy will take precedence. If all policies are user-defined, only the first policy will be converted.
- Supports conversion of IKEv2 with MSCHAPv2 only.
- Two-factor authentication (2FA) for VPN access is not supported due to design differences between uOS and ZLD
- IPsec VPN local/remote policy does not support address object types “range,” “interface-subnet,” “interface-IP,” or “interface-gateway,” and these cannot be converted.

DoS Prevention

- DoS Prevention conversion is not supported. The conversion may fail due to design structure differences.

Objects

- IPv6 objects are not supported for conversion.
- If the number of objects exceeds uOS limits, the conversion will fail. Please refer to the maximum object limits at Parameter section, back up your configuration, and manually reduce the number of objects before performing the conversion.
    - **Address Object**

ATP/USG FLEX 500	USG FLEX 500H
1000	500

ATP/USG FLEX 700	USG FLEX 700H
2000	1500

- **LDAP/ RADIUS/AD Server Object:**

• ATP/USG FLEX 200	USG FLEX 200H
8	4

ATP/USG FLEX 500	USG FLEX 500H
16	8

ATP/USG FLEX 700	USG FLEX 700H
16	8

- **LDAP/RADIUS/AD for each Group:**

ATP/USG FLEX 500	USG FLEX 500H
4	2

ATP/USG FLEX 700	USG FLEX 700H
4	2

- When the referenced object cannot be converted, the behavior in each feature's field will be as follows:
  - **Policy Control:**
    - If the rule references a Schedule Object, Zone Object, SSL Inspection Profile, or Content Filtering Profile, the rule will be set to the uOS default.
    - The rule will be converted with its status set to "Inactive," while the Address Object's Source and Destination fields, Service Object, and User Object will default to "any."
  - **Session Control:** Rules will be converted with their status set to "Inactive," and the Address Object and User Object will default to "any."
  - **Policy Route:**
    - Rules referencing an Interface in the "From" or "Next Hop" fields, or a Trunk (Interface Group), will not be converted and will be removed.
    - Rules referencing a Schedule Object will be set to the uOS default.
    - Rules will be converted with their status set to "Inactive." The Address Object's Source, Destination, and SNAT fields, along with the Service Object and User Object, will default to "any."
  - **Static Route**: Rules will be converted, and the Next Hop interface will remain the same as the ZLD settings. However, if the interface does not

exist in the uOS settings, users will need to create the interface manually to ensure the route functions properly.

- **DDNS:** If the DDNS primary interface cannot be converted, the profile will be removed. However, if the DDNS backup interface cannot be converted, it will be replaced with 'any'.
- **Trunk**: The trunk (interface group) will be converted but the member interface(s) will be removed. User have to modify the trunk by themselves.
- **Address Object:** If the address type is "Interface IP" or "Interface Subnet" or "Interface Gateway", it will not be converted and will be removed.
- **NAT Virtual-Server:**
  - Rules will be converted with their status set to "Inactive." The Address Object's Source and Destination fields, along with the Service Object will be set to default "any."
  - If the Interface or the port mapping Service/Service Group Object cannot be converted, the rule will be removed.
- **IP Exception:** If the Address Object in Source and Destination fields cannot be converted, the rule will be removed.

Users

- User types such as "guest," "guest-manager," "external group users," and "MAC address" are not converted. These must be manually created after the conversion.

Auth. Server

- HTTP authentication server will not be converted.
- If the AD/LDAP server password is shorter than four characters, change it to at least four before converting. Otherwise, the conversion will fail and the device may lose connection to Nebula.

Security Features

Some profiles or settings may be converted, but proper functionality is not guaranteed. Please review the logs and the converted configuration files carefully and make any necessary adjustments manually.

- **Content Filtering**:
  - For **DNS Content Filter** and **Web Content Filter** profiles, the system adds a prefix (**dns_** or **wcf_**) to the original profile name. If the combined name exceeds the 31-character limit, the original name is truncated to

25 characters and a two-character suffix (-0, -1, etc.) is appended for distinction.
    - The **Secure Policy only converts Web Content Filtering** (ZLD) settings to Content Filtering (uOS). Secure Policy settings for **DNS Content Filtering** (ZLD) will **not be converted**.
    - **DNS Safe Search settings are not supported** in the conversion process.
    - **Custom Service settings are not supported** in the conversion process.
    - ZLD **Allow List and Block List** are global settings, whereas uOS applies them per profile; therefore, Allow List and Block List settings **will not be converted**.

- **Anti-Malware:**
    - Anti-Malware settings are only **partially converted**. Since **uOS does not** support **Stream mode**, the converted configuration will include only the supported settings, and **Stream mode will be excluded**.
- **Application Patrol:**
    - Because ZLD does not support the multiple-application concept, the conversion tool groups ZLD applications into uOS multiple-application structures based on (action, log) combinations.
    - The converted settings may appear inconsistent or appear as “undefined” in the “Application” field of the uOS GUI Edit Application Patrol profile.
    - After conversion, additional manual adjustments or confirmations may be required to ensure that the converted profile/polices operate correctly.
- **IP Exception**: If the source or destination of the IP Exception profile is not set, the profile will not be converted.

- **SSL Inspection**:
    - uOS SSL Inspection does not support "Exclude List Web Category" settings; therefore, ZLD SSL Inspection Exclude List Web Category settings will not be converted.
    - Certificates and Licenses will not be migrated. Certificate will revert to using the uOS default certificate.

- **Security (UTM) Statistics**: Regardless of whether UTM Statistics was enabled or disabled in ZLD, after conversion it will be enabled in uOS.

SNMP

- SNMP Community Behavior – In uOS, the correct SNMP behavior requires the community value to exactly match the “Get” value, whereas ZLD does not enforce this validation.
- Only SNMP “Community” and “Get” values that match will be converted.

Unsupported Features for H Series

Some supported features will not be converted and will require users to manually configure them.

- 2FA authentication
- VPN Configure Provisioning
- ADP

Some features are not supported on current USG FLEX H series products and will be removed during the conversion process:

- Device High Availability (HA) configurations
- Captive Portal customization files and User Agreement portal files
- Hotspot configurations
- Secure WiFi, AP Controller

These features will never be supported on the H series and cannot be converted.

- L2TP/IPsec
- VPN Concentrator configurations
- Built-in WiFi configurations

LAG Interface Unsupported

LAG interface conversion is not supported. If the configuration includes a LAG interface, it will be removed during the conversion process.

Certificate Unsupported

CLI commands that reference a certificate will be modified to use the default certificate, as the original certificate will not exist on the target device.